Coordination of DERs in Microgrids with Cybersecure Resilient Decentralized Secondary Frequency Control

Hao Jan Liu, Matthew Backes, Richard Macwan, and Alfonso Valdes *
Department of ECE and ITI, University of Illinois at Urbana-Champaign
Emails: {haoliu6,mbackes2,rmacwan,avaldes}@illinois.edu

Abstract

Microgrids are emerging as an important strategy to advance resiliency of modern electric power systems. In this paper, a robust decentralized secondary frequency control design for islanded microgrids is developed to enable resilient coordination and integration of distributed energy resources (DERs). We cast the control problem centrally under steady state and adopt the feedback-based Alternating Direction Method of Multipliers (ADMM) algorithm for solving the decentralized control updates. The ADMM algorithm uses measurements at various points in the system to solve for control signals. Measurements and control commands are sent over communication networks such as Ethernet-based local area networks in the IEC 61850 standard. To enhance the robustness to cyber intrusions, we modify the ADMM algorithm using the Round-Robin technique to detect malicious DERs. As a complementary defense, an agreement algorithm based on a fast computation of Kirchhoff law conditions is implemented for continuously detecting false measurements. The results are demonstrated through simulation for a representative microgrid topology.

*The work described here was performed with funding from the Dept. of Energy (DOE) under Cooperative Agreement DE-OE0000831, under subcontract to ABB US Corporate Research Center. The views expressed are those of the authors. This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

1. Introduction

Grid modernization envisions the adoption of information and communication technologies in the electrical power system for measurement, state estimation, and control [1]. This enables the increasing penetration of distributed energy resources (DERs) in microgrids (MGs), defined as a collection of controllable loads, DERs, and controls to maintain stability and serve loads. MGs provide a framework for DER integration, optimization of local power systems, ability to serve critical loads, and the intelligence to recover after outages [2].

When connected to the AEPS, frequency regulation is provided by rotational inertia from legacy generation in the AEPS. In island mode, frequency regulation is a challenge because many DERs inherently have no rotational inertia. Thus, maintaining MG stability is the critical concern when inertia-less DERs, such as solar photovoltaic (PV) and a variety of battery and storage systems, are integrated in a network. Additionally, coupling DERs to the grid involves fast-acting power electronics inverters, requiring sophisticated embedded controllers for each resource [3]. Accordingly, accurate measurements at high sampling rates as well as control commands must be reliably delivered and trusted. To this end, the hierarchical control of DERs has recently been adopted as a standard operational paradigm for islanded MGs [4, 5]. The conventional droop control design, along with the faster inner voltage and current control loops, is implemented at the primary level. Such autonomous local droop control design aims to stabilize the system frequency and voltage under random disturbances while ensuring proportional power sharing among DERs that is proportional to the rated capacity of the DERs [6]. However, this primary control may lead to steady state mismatches from nominal frequency. Meanwhile, the secondary control design, enabled by the communication network, coordinates the system-wide information regarding the status of DERs to further minimize the mismatch error from the primary

URI: http://hdl.handle.net/10125/50226
ISBN: 978-0-9981331-1-9

level in a centralized fashion [7].

We formulate the secondary frequency control under steady state as a consensus optimization problem, as in [8]. To avoid a single point of failure and enhance DERs' plug-and-play capability, we propose to solve this problem in a decentralized fashion by adopting the Alternating Direction Method of Multipliers (ADMM) algorithm [9]. The ADMM is a splitting optimization technique that has been widely used in a variety of scientific disciplines such as signal processing, statistical learning, and more recently, power system operations [10]. Based on this algorithm, a DER controller uses local sensor measurements of voltage and current to perform a simple algorithmic computation for generating a local estimate. This estimate is then communicated to a central supervisor, which computes the average consensus of all estimates and broadcasts this consensus variable back to each DER controller. Our implementation differs from that of most decentralized frequency control designs [7, 11–13] in that we advocate modifying the ADMM updates originally derived for the steady state objective to an online feedback-based scheme, incorporating the instantaneous power measurements. Interestingly, it turns out that we do not need to explicitly model the MG power flow as the instantaneous power feedback signal couples DERs with power system networks. The proposed control design has been extensively validated using a realistic MG, and its performance can be guaranteed in terms of achieving zero frequency deviation with proportional power sharing among DERs.

While the cyber infrastructure enables the proposed decentralized control design, there is growing concern that it also exposes an attack surface for cyber adversaries. This is not hypothetical, as evidenced by recent cyber-induced outages in the Ukraine power system [14]. Hence, our control framework requires cyber defenses for controls and DERs against potential malicious cyber attacks. We consider an adversary model whereby an adversary can inject syntactically correct but destabilizing spoofed measurements and control commands, causing the secondary frequency control to fail and possibly resulting in an outage. The utilization of syntactically correct control commands during an attack to cause power outages has recently been reported [15], which motivates this work as addressing realistic attack scenarios.

Our contribution is to develop a *collaborative* defense strategy against these attacks by leveraging the communication capabilities under the IEC 61850 standard [16]. To enhance the robustness to malicious control command attacks, we employ the Round-Robin (RR) technique at the central supervisor for generating the consensus variable based on the ADMM algorithm [17]. Interestingly, by tracking the evolution of this RR-based variable, we are able to effectively identify compromised DER controllers. As for the measurement attack, we adopt a complementary defense based on an Agreement Algorithm (AA) to detect and locate false measurements on which the secondary control is based [18, 19]. It should be noted that these two approaches give visibility into where the attack is happening. Thus, this can not only enable appropriate response with the correct mitigation, but also can alert an operator to the *specific* root cause. Together with the RR and AA detection algorithms, the central supervisor would be able to either isolate the malicious communication links from control updates or trip the malicious DERs off-line. This provides a multi-pronged approach to resilient and efficient MG operation in the face of adversarial conditions. These algorithms are demonstrated through simulation analysis of several use cases of interest.

The remainder of this paper is organized as follows. Section 2 defines the reference MG topology and communication architecture, as well as attack scenarios. Section 3 introduces the droop control characteristic for islanded MGs while formulating the steady state consensus problem for the secondary control design. Section 4 develops the decentralized frequency control design by adopting the ADMM updates with the instantaneous power measurement feedback approach. Considering the attack scenarios in Section 2, we derive detection mechanisms and propose mitigation strategies in Section 5. Section 6 showcases the numerical results to validate our analytical claims. Concluding remarks are presented in Section 7.

2. Microgrid Modeling and Communication Architecture

In this section, we define a reference MG topology for this work and build a narrative around the attack scenarios. We also describe the IEC 61850 standard and its architecture which facilitates the control architecture design in Section 3. Additionally, we qualitatively detail the attack scenarios that the proposed mitigation strategies attempt to address.

2.1. Reference Microgrid Topology

Fig. 1 shows the reference topology considered in this paper. The MG is connected to the AEPS via a substation, with a corresponding POI where islanding decisions and requests can be executed. In normal operations the MG will be connected to the AEPS, but as a strategy for resilience, the MG has the ability to

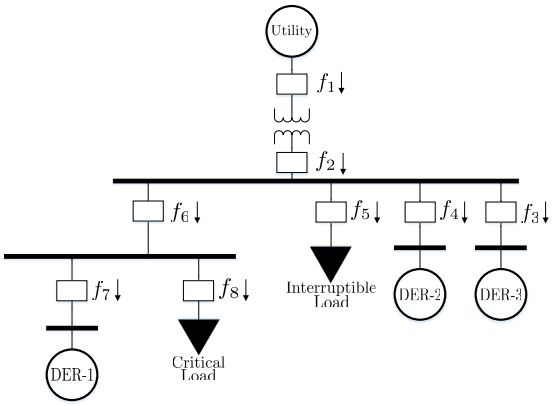

Figure 1. Reference microgrid topology for this work.

island from the AEPS in the event of an outage or other degraded operation, including cyber or physical attacks as well as widespread outage due to a major storm.

There are a variety of DERs and loads within the MG. Two DERs and an interruptible load are connected directly to the MG feeder head. The MG also contains a critical load and DER that essentially serves as the backup source dedicated to the critical load. With both critical load and DER buses, they have the ability to island themselves from the rest of the MG as a resilient strategy for the critical load. In effect, DER-1 and the critical load, with the associated bus, would become a nested microgrid.

2.2. Communication Architecture: IEC 61850

As communication networks continue to advance in electric power systems, an industry standard has emerged for metering, protection, and control functions. IEC 61850 provides a standard for configuring Intelligent Electronic Devices (IEDs) for electrical substation automation systems to be able to communicate with each other. It has since found applications in new domains, including MGs, see e.g., [20]. IEC 61850 defines a number of protocols for various classes of substation messages. Among the protocols relevant for our proposed MG control system are Sampled Values (SV) and Generic Object Oriented Sub- station Events (GOOSE). Sampled Values transmit digitized measurements of voltage and current from a merging unit to an IED. A merging unit accepts inputs from current transformers (CTs) and potential transformers (PTs), and produces digital, time-synchronized outputs communicated to other nodes via an Ethernet bus, known as the Process Bus in IEC 61850; see Fig. 2. GOOSE messages containing status, data, and control commands can be sent from one IED to another. The reason for

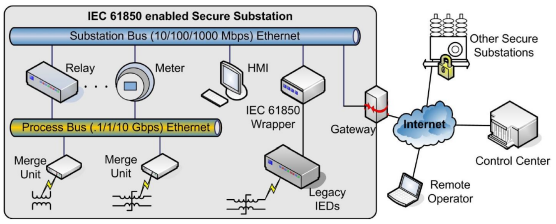

Figure 2. Notional representation of a standard IEC 61850 substation architecture.

introducing this architecture is two-fold. First, this standard is seeing increased applications in MGs, and as such, we find it relevant to design practical algorithms for field implementation. Second, using this standard provides a realistic attack surface that adversaries search out. We find it useful to provide specific solutions for a widely-used standard, especially considering a recent cyber attack impacting IEC 61850 [15]. Since we are dealing with MGs and not with bulk power systems, the number of nodes such as DER and other components is in the tens to at most low hundreds. Thus, modern substation communication architectures based on Ethernet are easily able to meet the transmission time and bandwidth requirements of the ensuing control architecture. As detailed soon, we consider malicious communication and control signal inputs which attempt to alter the MG operating points. Based on IEC 61850, such attacks can effectively drive the frequency away from the nominal, which is of extremely high stability concerns.

2.3. Attack Scenarios

Emerging MGs include a central MG controller, denoted in this paper as Microgrid Controller (MGC), which communicates with individual DER controllers. Measurements and commands travel over communication networks, as given by IEC 61850. This communication structure potentially exposes the system to cyber attack, which can assume the form of invalid commands (which can cause a DER to perform potentially destabilizing power injections) as well as falsified measurements (which can lead even a correctly functioning MGC to issue erroneous control commands).

2.3.1. Communication Link Attack on Control Command

The scenario is a communication link attack on the control command (not measurements) from the MGC which is used to exchange ADMM-related variables via the Ethernet-based IEC 61850 station bus. The attack would result in the MGC calculating the wrong

consensus variable, which would thus send the MG to a calculated off-nominal frequency setpoint. The attack detection mechanism examines the consensus variable and monitors for any rapid changes that exceed a threshold. If one is found, the mechanism looks for the errant local variable and sets the corresponding DER to local droop control. The remaining DERs participate in the secondary frequency control while the spoofed DER operates in local droop mode only.

2.3.2. Local Attack on DER Control Command

The second scenario considers a local control command attack. An attacker compromises the DER controller by some mechanism. The attacker can then cause the system frequency and consensus variable to deviate from the appropriate references. This attack detection again relies on monitoring the consensus variable. Therefore, when it detects which DER is malicious, it again sets the malicious DER to local control mode since it is not yet known if it is a communication link or local controller attack at this point. By setting the malicious DER to local droop mode, if the system frequency and consensus variable are not converging to reference setpoints after a short time period, the MGC then determines such attack must be a local DER controller attack and issues a trip signal to the relay connecting the DER unit to the MG.

2.3.3. Local Measurement Attack

For the last attack scenario, we assume that the attacker has access either locally to the merging unit (the sensor), or can have access to the Ethernet-based process bus and is thus able to inject false measurement data. The DER controller that subscribes to the measurement messages would thus calculate incorrect power injection commands due to the faulty measurements. This could drive the MG to an unstable state. We assume that the attack is large enough to cause a reasonable frequency disturbance within the MG. Accordingly, a local merging unit attack may result in the tripping of the DER while a communication link attack on data measurements leads to reconfigure the control algorithm and exclude the malicious DERs by setting them to the local droop mode. We next present the secondary frequency control problem statement with the proposed ADMM-based solver and Round-Robin-based detection mechanism.

3. System Modeling and Problem Statement

The islanded MG consists of m buses, where the buses in $\mathcal{N} := \{1, \cdots n\}$ are DER buses and the rest are in the subset of load buses $\mathcal{N}_L := \{n+1, \cdots m\}$. Per bus-$i$, we represent the complex voltage and its phase angle as v_i and θ_i, respectively. The active power injection of DER-i is denoted by P_i while P_i^* corresponds to its active power rating. Additionally, $\omega_i := (\dot{\theta}_i - \omega_b)$ is the frequency deviation with $\dot{\theta}_i := d\theta_i/dt$ and ω_b representing the frequency and nominal frequency set-point, respectively. To facilitate the ensuing control design, we introduce the following assumptions that are commonly used in the microgrid literature [8, 21, 22].

(A1) The power lines are relatively short and thus lossless.

(A2) The voltage magnitude $|v_i|$ at each bus is regulated to stay constant.

(A3) All possible load variations can be fully supported by the DERs without violating their active power rating limits.

(A4) The load stays constant and is independent of frequency while executing the proposed frequency control.

The short distance property in (A1) typically holds for power lines in MGs. Hence, line losses are negligible compared to line flows. Through the fast inner control loops along with the voltage-droop control design, DERs' reactive power output is used to track a reference voltage level, at a much faster time-scale than that of the frequency control. This time-scale separation between frequency and voltage dynamics is well supported by earlier work on MG modeling [23]. Accordingly, this leads to (A2) where the voltage magnitude at all nodes can be assumed to be fixed (see, e.g., [4, 21, 22]). Additionally, (A3) can be guaranteed through a careful system planning at the MG deployment stage; see e.g., [24, Remark 1]. Last, under a load disturbance, the proposed frequency control design is fast enough to restore the system frequency to its nominal value before another load change occurs. Additionally, the frequency independent load assumption in (A4) is needed for developing and analyzing the proposed control design. It is true that there could exist different types of loads in MGs, such as the prior work in [22, 25] which has considered frequency dependent loads. Motivated by [25], it is potentially feasible to generalize the proposed control design to include frequency dependent loads. This direction will be pursued in future work.

The goal of a secondary frequency control is to 1) ensure a steady state zero frequency deviation (i.e., $\omega_i = 0, \forall i$) and 2) guarantee autonomous active power sharing

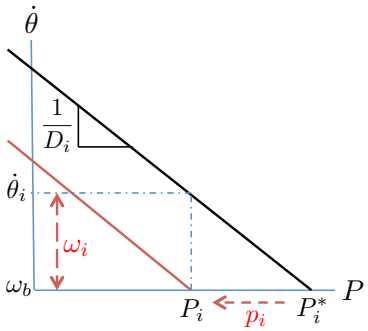

Figure 3. Frequency droop characteristics with proposed secondary control design.

in proportion to active power ratings among all DERs such that

$$\frac{P_1}{P_1^*} = \frac{P_2}{P_2^*} = \cdots \frac{P_n}{P_n^*}.$$

To this end, the active power-frequency (P-ω) droop control is adopted to achieve these objectives [26]. Fig. 3 depicts the droop characteristics which mimics the dynamical swing equation of a synchronous generator with zero machine inertia, as given by

$$D_i\omega_i = P_i^* - P_i - p_i \tag{1}$$

where the droop coefficient D_i is determined by the rating of DER-i. Herein we set a uniform D_i/P_i^* among all DERs. Compared to conventional P-ω droop control, an additional control input p_i is introduced in (1). Since P_i^* and D_i are fixed parameters, the operating set-point of DER-i can only be changed by judiciously controlling p_i. Under (A2), the model (1) holds because of the decoupled dynamics between frequency and voltage control. Accordingly, the frequency will be controlled by adjusting the active power only assuming voltage magnitudes stay constant [4, 21, 22].

Upon concatenating all scalar variables into vector form, we formulate the secondary control problem as a consensus optimization problem, as given by

$$\begin{aligned} &\min_{\mathbf{p}} \ \|\mathbf{P}^* - \mathbf{P} - \mathbf{p}\|^2_{\mathbf{D}^{-1}} \\ &\text{subject to } \frac{p_i}{D_i} = \frac{p_j}{D_j}, \ \forall i, j \in \mathcal{N} \end{aligned} \tag{2}$$

where $\mathbf{D} := \text{diag}(D_1, ...D_n)$ is an $n \times n$ diagonal matrix and the weighted norm $\|\mathbf{v}\|^2_{\mathbf{D}} := \mathbf{v}^T\mathbf{D}\mathbf{v}$ for any vector $\mathbf{v}$. Under steady state and (A3), the objective of (2) turns out to be zero, corresponding to achieving a zero system frequency deviation. In addition, due to a uniform D_i/P_i^*, the equality constraints in (2) equivalently enforce a proportional active power sharing. Note that the quadratic program (2) could be solved using off-the-shelf convex solvers. Nonetheless, the challenge lies in that the active power injection $\mathbf{P}$ is dynamical and coupled to the power system network. To tackle this problem, we adopt the feedback approach from [8] to account for system dynamics. We refer the reader therein for detailed derivations. To sum up, under (A1)-(A4), the optimizer of (2) can effectively archive the aforementioned goal of secondary frequency regulation.

4. ADMM-based Decentralized Solver

This section introduces our proposed ADMM-based decentralized secondary control design. The dynamics coupling $\mathbf{P}$ and $\mathbf{p}$ are neglected initially. As detailed below, the feedback approach will be introduced to account for such interactions. Hence, the objective in (2) is fully separable. Using the IEC 61850 communication protocol for measurement and control messages, we can solve the consensus optimization problem (2) in a fully decentralized fashion. For notational convenience, we let the optimization variable $x_i := p_i/D_i$ and the input variable $c_i := (P_i^* - P_i)/D_i$ where P_i is the active power injection from DER-i and locally measurable. Accordingly, (2) can be reformulated as

$$\underset{\mathbf{x},z}{\text{minimize}} \ \ \frac{1}{2}\|\mathbf{c} - \mathbf{x}\|^2_{\mathbf{D}} \tag{3a}$$

$$\text{subject to} \ \ \mathbf{x} = z\mathbf{1} \tag{3b}$$

where z is a consensus value among the DERs. Note that the equality constraints in (2) are equivalent to (3b) under a connected communication network. Defining the multipliers $\boldsymbol{\lambda}$ and a constant $\rho > 0$, we introduce the augmented Lagrangian function as $\mathcal{L} = \sum_{\forall i \in \mathcal{N}} \mathcal{L}_i(x_i, z, \lambda_i)$ where

$$\mathcal{L}_i(x_i, z, \lambda_i) = \frac{D_i}{2}(c_i - x_i)^2 + \lambda_i(x_i - z) + \frac{\rho}{2}(x_i - z)^2. \tag{4}$$

Based on the (4), the ADMM algorithm is invoked and its $(k+1)$-st iteration for DER-i has the following three steps [9]:

(S1) Update $\mathbf{x}$: As $\mathcal{L}$ totally decouples into $\mathcal{L}_i$ for each DER-i, minimizing x_i involves only the variables z^k and λ_i^k. Thus, upon receiving z^k from the MGC, the update is

$$x_i^{k+1} := \arg\min_{x_i} \ \ \mathcal{L}_i(x_i, z^k, \lambda_i^k). \tag{5}$$

Taking the gradient of $\mathcal{L}_i$ with respect to x_i and

setting it to zero, we have

$$x_i^{k+1} = \frac{\rho z^k + D_i c_i^k - \lambda_i^k}{D_i + \rho} \tag{6}$$

where c_i^k is the feedback measurement signal, corresponding to the active power injection of DER-i.

(S2) Update $\mathbf{z}$: Likewise, the consensus variable is updated as

$$z^{k+1} := \arg\min_z \ \mathcal{L}(\mathbf{x}^{k+1}, z, \boldsymbol{\lambda}^k).$$

By initializing $\boldsymbol{\lambda}^0 = \mathbf{0}$, the summation $\sum_{i\in\mathcal{N}} \lambda_i^{k+1}$ is guaranteed to stay zero. Thus, we have

$$z^{k+1} = \frac{\sum_{i=1}^n x_i^{k+1}}{|\mathcal{N}|}. \tag{7}$$

(S3) Update $\boldsymbol{\lambda}$: Each multiplier is linearly updated by the iterative mismatch of the constraint (3b), as given by

$$\lambda_i^{k+1} = \lambda_i^k + \rho(x_i^{k+1} - z^{k+1}). \tag{8}$$

Because $\boldsymbol{\lambda}^0 = \mathbf{0}$, we have

$$\sum_{i\in\mathcal{N}} \lambda_i^{k+1} = \rho \sum_{i\in\mathcal{N}} \sum_{t=1}^{k+1} (x_i^t - z^t) = 0.$$

This fact corroborates the derivation in (7).

5. Detection and Localization Strategies

Under IEC 61850 communication network, we assume that attackers have compromised the local DER controllers such that the local variable $\mathbf{x}$ is altered, e.g., $\bar{x}_i^{k+1} = x_i^{k+1} + \delta_i^{k+1}$ where δ_i^{k+1} is the bias appended to x_i^{k+1} at the DER-i. Therefore, z^{k+1} in (7) at the MGC becomes

$$z^{k+1} = \frac{\sum_{i=1}^n (x_i^{k+1} + \delta_i^{k+1})}{n} = \Delta^{k+1} + \frac{\sum_{i=1}^n x_i^{k+1}}{n} \tag{9}$$

with $\Delta^{k+1} := \frac{\sum_{i=1}^n \delta_i^{k+1}}{n}$ being the average attack bias signal with time-varying and arbitrary magnitude. Under the presence of this attack, the consensus variable z^{k+1} would diverge unless Δ^{k+1} is designed specifically so the effect on the consensus variable is trivial. This is, however, unlikely to happen as the attacker does not have the full system information. In any case, such an attack bias signal may drive the MG to unstable conditions and/or damage system equipment, e.g., causing divergence of z^{k+1}.

It is imperative to detect and localize the malicious attack signals promptly since the control design is based on z^{k+1}. To this end, we monitor the evolution of z^{k+1} and design a flag to trigger the ensuing detection algorithm. Assuming the convergence of z^{k+1} after $k^\star$ iterations, we would trigger the detection algorithm once the following condition has been satisfied:

$$|z^{k+1} - z^k| > \epsilon$$

where $\epsilon > 0$ is a pre-defined threshold.

5.1. Round-Robin-Based ADMM Detection Algorithm

The RR-ADMM detection algorithm to discover the malicious DERs is adapted from [17]. The RR is an arrangement of selecting the DER in a fixed rational order, i.e., DER-1, DER-2, ..., DER-n. For notational convenience, we denote the consensus variable for the RR-ADMM at iteration k as $\tilde{z}^k$. Given $\alpha > 0$, the steps (S1)-(S3) become

$$\mathbf{x}^{k+1} = (\mathbf{D} + \rho\mathbf{I})^{-1}(\rho\tilde{z}^k\mathbf{1} + \mathbf{D}\mathbf{c}^k - \boldsymbol{\lambda}^k), \tag{10a}$$

$$\tilde{z}^{k+1} = \alpha(x_{\tilde{i}}^{k+1} + \delta_{\tilde{i}}^{k+1}), \tag{10b}$$

$$\boldsymbol{\lambda}^{k+1} = \boldsymbol{\lambda}^k + \rho(\mathbf{x}^{k+1} - \tilde{z}^{k+1}\mathbf{1}) \tag{10c}$$

where $\mathbf{I}$ is the identity matrix with $\tilde{i} = 1, \cdots, n$ representing the fixed Round-Robin iteration index. For a non-malicious DER, we set $\delta_{\tilde{i}}^{k+1} = 0$. Hence, we have the consensus variable $\tilde{z}^{k+1}$ as

$$\tilde{z}^{k+1} = \alpha\delta_{\tilde{i}}^{k+1} + \alpha\frac{\rho\tilde{z}^k + D_{\tilde{i}}c_{\tilde{i}}^k - \lambda_{\tilde{i}}^k}{D_{\tilde{i}} + \rho}. \tag{11}$$

For $k \geq 1$, (11) can be expressed as

$$\tilde{z}^{k+1} = \alpha\delta_{\tilde{i}}^{k+1} + \alpha\frac{\rho\tilde{z}^k + D_{\tilde{i}}c_{\tilde{i}}^k - \rho\sum_{t=1}^k (x_{\tilde{i}}^t - \tilde{z}^t)}{D_{\tilde{i}} + \rho}. \tag{12}$$

Let $\tilde{\mathbf{z}}_r := \{\tilde{z}_{r,1}, \cdots, \tilde{z}_{r,n}\} \in \mathbb{R}^n$ gather the all the values of the consensus variable at the r-th round of the RR-ADMM algorithm. To determine a threshold to separate malicious DER controllers from the rest of

Algorithm 1 Detection and Localization Strategies

for every iteration $k = 0, 1, 2, \cdots$ **do**
  for $i \in \mathcal{N}$ **do**
    Compute x_i^{k+1} as in (6) and send it to MGC
  end for
  MGC computes z^{k+1} as in (7)
  if $|(z^{k+1} - z^k| > \epsilon) \wedge (k > k^\star)$ **then**
    if $r = 1$ **then**
      MGC computes $\tilde{z}^{k+1}$ as in (10b)
      Broadcast the value of $\tilde{z}^{k+1}$ to all DERs
      Determine the index $\tilde{n}$ for the minimum entry of $\tilde{z}_1$
    end if
    if $(r = 2) \wedge (k \leq k^\star + n + \tilde{n})$ **then**
      MGC computes $\tilde{z}^{k+1}$ as in (10b)
      Broadcast the value of $\tilde{z}^{k+1}$ to all DERs
      Identify malicious DER-$\tilde{i}$ where $\{\tilde{i} \mid \tilde{z}_{1,\tilde{i}} > \tilde{z}_{2,\tilde{n}}, \forall \tilde{i} \in \mathcal{N} \setminus \tilde{n}\}$
      MGC reconfigures the communication network, resets $\boldsymbol{\lambda}^k = \mathbf{0}$, and/or trip malicious DERs off-line
    end if
  else
    Broadcast the value of z^{k+1} to all DERs
  end if
  for $i \in \mathcal{N}$ **do**
    Compute λ_i^{k+1} as in (8)
  end for
end for

the system, we assume that the bias $\delta_{\tilde{i}}^{k+1}$ is sufficiently large enough. Based on (12), one of the values from the non-malicious DERs during the r-th round must be $\tilde{z}_{r,\tilde{n}}$ with the index $\tilde{n}$ corresponding to the smallest element of $\tilde{\mathbf{z}}_r$. Given this index, the $(r+1)$-st round is carried out for obtaining the value of $\tilde{z}_{r+1,\tilde{n}}$ where $\tilde{n}$ is the same index as round 1, and this serves as the detection threshold. Hence, any $\tilde{z}_{r,\tilde{i}} > \tilde{z}_{r+1,\tilde{n}}, \forall \tilde{i} \in \mathcal{N} \setminus \tilde{n}$ is identified as the malicious DER in the MG. For a given initialization time index $k^\star$, Algorithm 1 tabulates the detection strategy. As for the localization strategy to isolate the aforementioned malicious attack signals, the MGC first reconfigures the communication network so the malicious DERs no longer participate the ADMM updates in (S1)-(S3) and thus switch to only local droop (primary) control mode. Meanwhile, if zero frequency deviation is achieved, we conclude the isolation process. Otherwise, the malicious DERs are tripped off-line because of either measurement or control signal attack. Last, note that there must be at least one non-malicious DER in the system for the RR-ADMM detection scheme to work. Such a scheme is only for detection purposes. Thus, once the malicious attacks are localized, the control design is reverted back to follow the ADMM algorithm in (S1)-(S3).

5.2. Measurement Attack Detection

We now describe a defense against false measurement injection to complement defenses against control attacks given above. We adopt the Agreement Algorithm (AA), which was developed in [18], to determine and locate malicious measurement attacks on substation IEDs and controllers. Accordingly, assuming the loads as constant impedances, the Kirchhoff's voltage and current laws along with Ohm's law are used to facilitate the development of agreement matrix $\mathbf{A}$ for a particular topology. Albeit we assume loads as constant impedance, a general assumption in power flow studies, the method for developing the AA presented herein remains valid for other load models. Elements of $\mathbf{A}$ corresponding to the currents reflect the signed topology of the corresponding merging unit while others corresponding to voltages are reciprocal complex impedances on the corresponding lines. Fig. 1 showcases the reference MG topology with corresponding measurement locations. The polarity of the complex current f_i measured at i-th merging unit is positive when current flows *into* the loads and DERs. By concatenating as $\mathbf{x} = (\mathbf{f}, \mathbf{v})$, the physical equation can be rewritten as

$$\mathbf{A}\mathbf{x} = \mathbf{0}. \tag{13}$$

Considering that (13) is similar to the error correcting code formulation from [18], if an attacker falsifies one of the measurements, we would have a non-zero corresponding element of the resultant vector, known as the Syndrome vector. By injecting the malicious vectors $\Delta\mathbf{f}$ and $\Delta\mathbf{v}$ to the measurements, we have $\bar{\mathbf{x}} = (\mathbf{f} + \Delta\mathbf{f}, \mathbf{v} + \Delta\mathbf{v})$. Thus, the Syndrome vector is

$$\mathbf{s} = \mathbf{A}\bar{\mathbf{x}}. \tag{14}$$

By observing the pattern of vector $\mathbf{s}$, we can classify multiple subsets of potential malicious merging units. Accordingly, the largest magnitude element of a subset corresponds to the malicious location. This detection mechanism is valid for a limited number of attacks. We refer the reader to [19] for a detailed discussion.

6. Numerical Tests

In this section, we evaluate the proposed mitigation strategies and responses for the communication and measurement link attack scenarios. The three-phase MG topology and power system parameters are given in Fig.

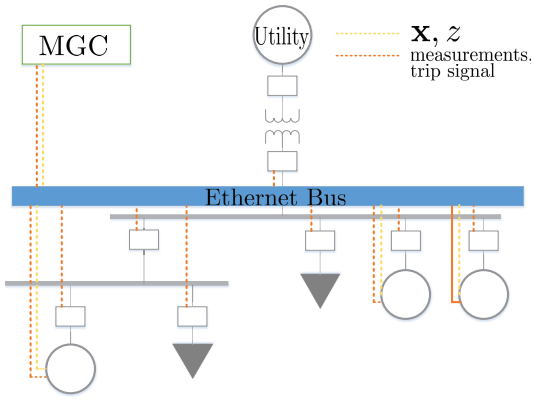

Figure 4. Reference microgrid communication architecure and data types.

1. The load is modeled as a constant impedance load, which is frequency independent. Fig. 4 depicts the MG control system communication network topology. To reiterate, the measurements are sent to the local DERs from a merging unit (which we omit from the figure), and the DERs and MGC communicate updates for the ADMM algorithm. This is done over switched Ethernet, denoted by the Ethernet bus in Fig. 4. All numerical tests are performed in Mathworks® MATLAB 2013a and Simulink software.

6.1. Load Perturbations

In this scenario, we increase the system load by 100% at t = 4s. Each DER is rated at $P_i^* = 1500$ W, $\forall i$, and we let $D_i = 5 \times 10^4$ W.s.rad^{-1}, $\forall i$ to satisfy the active power sharing. The ADMM algorithm is executed every 100 ms with $\rho = 1 \times 10^5$. The resulting bus frequencies and active power output are shown in Fig. 5. Within approximately 1.5 seconds, the secondary frequency control is able to obtain zero system frequency deviation from nominal, and the DERs have correctly achieved equal power sharing. Accordingly, each DER archives the the steady state frequency of 60 Hz.

6.2. Local Attack on DER Controller

We generate an attack signal as a time-varying random number from a uniform (0,3) distribution and draw a new random value at a time step of 100 ms. We multiply this by the steady state x_i value at the attack location, so that the attack is effectively a random re-scaling of this value. Given the steady state conditions, the attack is introduced at t = 4.1s on the local x_i issued to DER-3. The resulting system response and RR-ADMM attack detection and

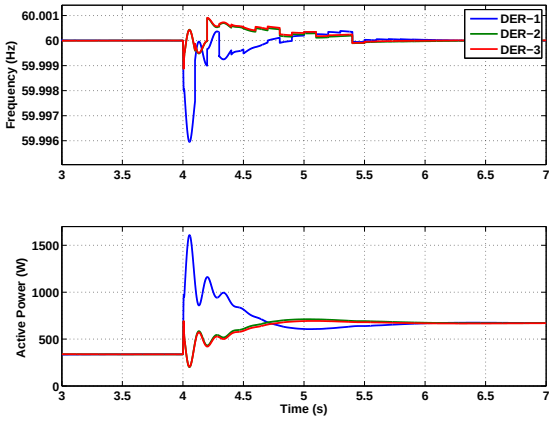

Figure 5. Frequency and active power output response to a load disturbance.

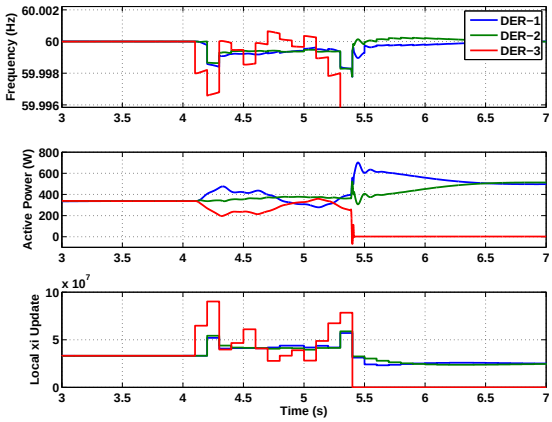

Figure 6. Frequency, active power output, and local x_i update responses to a local controller attack in steady state operation.

mitigation algorithm results are shown in Fig. 6. From the plot of the local x_i update, this particular attack introduces a signal that is approximately 275% of the steady state x_3 signal. Clearly, the system diverges away from its steady state while the attack is present. At t = 5.4s with ϵ setting at 10% of the steady state x_3 signal, the RR-ADMM algorithm successfully detects DER-3 as malicious and trips it off-line, i.e., $P_3 = 0$. For t > 5.5s, the ADMM algorithm changes to only include DER-1 and DER-2, achieving the nominal frequency of 60 Hz.

Next, we investigate the effectiveness of the RR-ADMM detection algorithm for an attack during a load disturbance. While a coincidental simultaneous occurrence of these two events may seem unlikely, we are motivated to seek solutions to coordinated attacks, i.e., the attacker causes a load disruption *and* alters

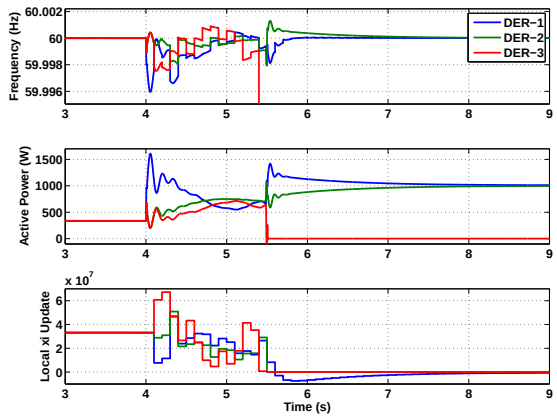

Figure 7. Frequency, active power output, and local x_i update responses to a local controller attack during a load disturbance.

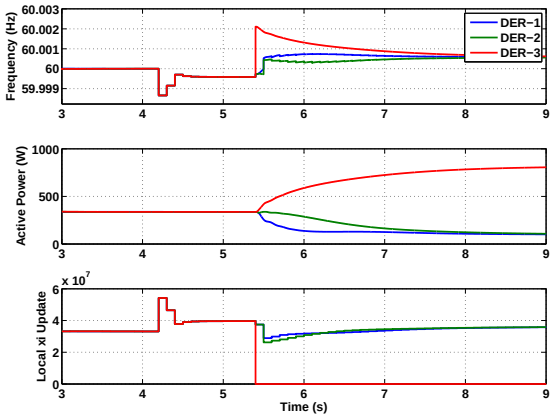

Figure 8. Frequency, active power output, and local x_i update responses to an communication link attack on a control command.

the local controller updates, as depicted in Fig. 7. At t = 4s, we introduce a load disturbance of 25% and then subsequently cause an attack at t = 4.1s on the x_i update to DER-3, similar to the attack scenario in the steady state case. We see that the random attack signal is approximately 200% of the transient x_3 signal. The RR-ADMM algorithm is still able to identify the malicious DER even in the presence of a load disturbance. After reconfiguring the ADMM algorithm and tripping DER-3 off-line at t = 5.5s, the system achieves the nominal frequency of 60 Hz.

6.3. Communication Link Attack on Control Command

We consider that an attacker has gained access to the station bus (Ethernet bus) that is exchanging control commands between the local DER controllers and the MGC. The attacker is able to spoof the MAC address of a DER controller and thus can alter control commands over the link. This is contrasted with the previous attack since it is not on the local DER controller, and thus the time-varying attack signal does not directly affect the power injection command to the DER. The attack detection monitors the consensus variable and raises a flag when a deviation occurs that exceeds a threshold. In our simulation, we again use a 10% deviation as the threshold. As the consensus variable is the average across n DERs, an attack bias may not be large, so that is the motivation for setting a relatively sensitive ϵ. After the flag is raised, the RR-ADMM is executed to determine which DER is malicious. The MGC then reconfigures the ADMM update to only include the non-malicious DERs while issuing a configuration command to the spoofed DER to revert to local frequency droop control. The spoofed DER should then eventually return to its initial power setpoint while the non-malicious ones continue to regulate the system frequency for achieving 60 Hz. Fig. 8 depicts the results of this attack scenario. At t = 4.1s, an attack signal is introduced on the x_3 update sent from DER-3 controller to the MGC. With the same random attack signal, the MGC then runs the detection mechanism from the RR-ADMM to find the malicious DER. At t = 5.3s, the MGC identifies that DER-3 is malicious and removes it from the ADMM update by setting it to local frequency control mode. Note that the x_3 update is a function of p_3, which is the power injection offset to the droop curve in Fig. 3. By setting x_3 to zero, the corresponding DER controller equivalently becomes the local droop control. By reconfiguring the ADMM algorithm, the DER-1 and DER-2 continue to execute the secondary frequency control while maintaining power sharing and achieving the nominal frequency of 60 Hz.

7. Conclusions

In this paper, we introduce a decentralized secondary frequency control that can successfully achieve frequency regulation in islanded ac microgrids. This approach is based on formulating the DER droop characteristic equations as a consensus optimization problem with a power injection offset command as the control variable. This quadratic program is solved with an ADMM-based decentralized algorithm. To this end, DER controllers locally compute their power injection offsets and communicate these values with the central controller, which then calculates the consensus of all DERs and broadcasts over the network. This decentralized approach allows for cyber attack detection mechanisms on local controllers and

communication link attacks. The proposed detection algorithm is based on a Round-Robin ADMM algorithm which sequentially updates the consensus variable as a function of local controller updates to identify malicious DERs. We pair this with a so-called agreement algorithm, a complementary false data injection detection mechanism. Mitigation strategies such as isolating attackers from the control algorithm or tripping a compromised DER off-line entirely are discussed. Together with these algorithms, we can implement a cybersecure resilient closed-loop control architecture. Finally, we demonstrate the effectiveness of our decentralized secondary frequency control design and detection algorithms using three case studies.

References

[1] J. A. Momoh, "Smart grid design for efficient and flexible power networks operation and control," in *2009 IEEE/PES Power Systems Conference and Exposition*, pp. 1–8, March 2009.

[2] N. Hatziargyriou, H. Asano, R. Iravani, and C. Marnay, "Microgrids," *IEEE Power and Energy Magazine*, vol. 5, pp. 78–94, July 2007.

[3] J. M. Guerrero, J. C. Vasquez, J. Matas, L. G. de Vicuna, and M. Castilla, "Hierarchical control of droop-controlled ac and dc microgrids - a general approach toward standardization," *IEEE Transactions on Industrial Electronics*, vol. 58, pp. 158–172, Jan 2011.

[4] J. W. Simpson-Porco, F. Dörfler, and F. Bullo, "Synchronization and power sharing for droop-controlled inverters in islanded microgrids," *Automatica*, vol. 49, pp. 2603–2611, Sept. 2013.

[5] F. Dörfler, J. Simpson-Porco, and F. Bullo, "Breaking the hierarchy: Distributed control & economic optimality in microgrids," *IEEE Trans. Control Netw. Syst.*, vol. 3, pp. 241–253, Sept 2016.

[6] F. Katiraei and M. R. Iravani, "Power management strategies for a microgrid with multiple distributed generation units," *IEEE Trans. Power Syst.*, vol. 21, pp. 1821–1831, Nov 2006.

[7] J. W. Simpson-Porco, Q. Shafiee, F. Dörfler, J. C. Vasquez, J. M. Guerrero, and F. Bullo, "Secondary frequency and voltage control of islanded microgrids via distributed averaging," *IEEE Trans. Ind. Electron.*, vol. 62, pp. 7025–7038, Nov 2015.

[8] L. Y. Lu, H. J. Liu, and H. Zhu, "Distributed secondary control for isolated microgrids under malicious attacks," in *2016 North American Power Symposium (NAPS)*, pp. 1–6, Sept 2016.

[9] S. Boyd, N. Parikh, E. Chu, B. Peleato, and J. Eckstein, "Distributed optimization and statistical learning via the alternating direction method of multipliers," *Found. Trends Mach. Learn.*, vol. 3, pp. 1–122, Jan. 2011.

[10] H. J. Liu, W. Shi, and H. Zhu, "Distributed voltage control in distribution networks: Online and robust implementations," *IEEE Transactions on Smart Grid*, 2017. (to be published).

[11] A. Bidram, A. Davoudi, F. L. Lewis, and J. M. Guerrero, "Distributed cooperative secondary control of microgrids using feedback linearization," *IEEE Transactions on Power Systems*, vol. 28, pp. 3462–3470, Aug 2013.

[12] L. Y. Lu and C. C. Chu, "Consensus-based secondary frequency and voltage droop control of virtual synchronous generators for isolated ac micro-grids," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 5, pp. 443–455, Sept 2015.

[13] L. Y. Lu and C. C. Chu, "Consensus-based droop control of isolated micro-grids by admm implementations (to be published)," *IEEE Transactions on Smart Grid*, 2017.

[14] R. Lee, M. Assante, and T. Conway, "Analysis of the cyber attack on the Ukrainian power grid," E-ISAC Report, March 2016.

[15] R. Lee, "CRASHOVERRIDE: Analysis of the threat to electric grid operations," Dragos Inc., March 2017.

[16] "Communication networks and systems for power utility automation - all parts."

[17] M. Liao and A. Chakrabortty, "Optimization algorithms for catching data manipulators in power system estimation loops," *CoRR*, vol. abs/1608.00299, 2016.

[18] A. Valdes, C. Hang, P. Panumpabi, N. Vaidya, C. Drew, and D. Ischenko, "Design and simulation of fast substation protection in IEC 61850 environments," in *2015 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, pp. 1–6, April 2015.

[19] R. Macwan, C. Drew, P. Panumpabi, A. Valdes, N. Vaidya, P. Sauer, and D. Ishchenko, "Collaborative defense against data injection attack in IEC 61850 based smart substations," in *2016 IEEE Power and Energy Society General Meeting (PESGM)*, pp. 1–5, July 2016.

[20] A. Ruiz-Alvarez, A. Colet-Subirachs, F. A.-C. Figuerola, O. Gomis-Bellmunt, and A. Sudria-Andreu, "Operation of a utility connected microgrid using an IEC 61850-based multi-level management system," *IEEE Transactions on Smart Grid*, vol. 3, pp. 858–865, June 2012.

[21] M. Zholbaryssov and A. D. Dominguez-Garcia, "Distributed enforcement of phase-cohesiveness for frequency control of islanded inverter-based microgrids," *IEEE Trans. Control Netw. Syst.*, 2017. (to be published).

[22] S. T. Cady, A. D. Domínguez-García, and C. N. Hadjicostis, "A distributed generation control architecture for islanded AC microgrids," *IEEE Trans. Control Syst. Technol.*, vol. 23, pp. 1717–1735, Sept 2015.

[23] J. Schiffer, D. Zonetti, R. Ortega, A. M. Stanković, T. Sezi, and J. Raisch, "A survey on modeling of microgrids-from fundamental physics to phasors and voltage sources," *Automatica*, vol. 74, pp. 135–150, Dec. 2016.

[24] X. Wu, C. Shen, and R. Iravani, "A distributed, cooperative frequency and voltage control for microgrids," *IEEE Trans. Smart Grid*, 2017. (to be published).

[25] C. Zhao, U. Topcu, N. Li, and S. Low, "Design and stability of load-side primary frequency control in power systems," *IEEE Trans. Autom. Control*, vol. 59, pp. 1177–1189, May 2014.

[26] M. C. Chandorkar, D. M. Divan, and R. Adapa, "Control of parallel connected inverters in standalone AC supply systems," *IEEE Trans. Ind. Appl.*, vol. 29, pp. 136–143, Jan 1993.